AF/$
JFW

PATENT
Attorney Docket No. 09812.0583-00

BEFORE THE BOARD OF PATENT APPEALS AND INTERFERENCES

In re Application of:	)	
	)	
Yoshihito ISHIBASHI et al.	)	Group Art Unit: 2165
	)	
Application No.: 09/396,054	)	Examiner: Neveen ABEL JALIL
	)	
Filed: September 15, 1999	)	Confirmation No.: 6914
	)	
For: CONTENT MANAGEMENT METHOD, AND CONTENT STORAGE SYSTEM	)	

Mail Stop Appeal Brief--Patents
Commissioner for Patents
P.O. Box 1450
Alexandria, VA 22313-1450

Sir:

TRANSMITTAL OF APPEAL BRIEF (37 C.F.R. 41.37)

Transmitted herewith is the APPEAL BRIEF in this application with respect to the Notice of Appeal filed on September 5, 2006.

This application is on behalf of

☐ Small Entity ☒ Large Entity

Pursuant to 37 C.F.R. 41.20(b)(2), the fee for filing the Appeal Brief is:

☐ $250.00 (Small Entity)

☒ $500.00 (Large Entity)

TOTAL FEE DUE:

Appeal Brief Fee	$500.00
Extension Fee (if any)	$0
Total Fee Due	$500.00

☒ Enclosed is a check for $500.00 to cover the above fees.

PETITION FOR EXTENSION. If any extension of time is necessary for the filing of this Appeal Brief, and such extension has not otherwise been requested, such an extension is hereby requested, and the Commissioner is authorized to charge necessary fees for such an extension to our Deposit Account No. 06-0916. A duplicate copy of this paper is enclosed for use in charging the deposit account.

FINNEGAN, HENDERSON, FARABOW,
GARRETT & DUNNER, L.L.P.

Dated: November 3, 2006

By: _____
Reece Nienstadt
Reg. No. 52,072

PATENT
Attorney Docket No. 09812.0583-00

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

In re Application of:	)	
	)	
Yoshihito ISHIBASHI et al.	)	Group Art Unit: 2165
	)	
Application No.: 09/396,054	)	Examiner: Neveen ABEL JALIL
	)	
Filed: September 15, 1999	)	Confirmation No.: 6914
	)	
For: CONTENT MANAGEMENT METHOD, AND CONTENT STORAGE SYSTEM	)	

Mail Stop Appeal Brief--Patents
Commissioner for Patents
P.O. Box 1450
Alexandria, VA 22313-1450

Sir:

APPEAL BRIEF UNDER BOARD RULE § 41.37

In support of the Notice of Appeal filed September 5, 2006, and further to Board Rule 41.37, Appellants present this brief and enclose herewith a check for the fee of $500.00 required under 37 C.F.R. § 1.17(c).

This Appeal responds to the June 5, 2006, final rejection of claims 1-41.

If any additional fees are required or if the enclosed payment is insufficient, Appellants request that the required fees be charged to Deposit Account No. 06-0916.

Table of Contents

I. REAL PARTY IN INTEREST

Sony Corporation is the real party in interest.

II. RELATED APPEALS AND INTERFERENCES

There are currently no other appeals or interferences, of which Appellants, Appellants' legal representative, or Assignee are aware, that will directly affect or be directly affected by or have a bearing on the Board's decision in the pending appeal.

III. STATUS OF CLAIMS

Claims 1-41 are currently pending in this application and have been finally rejected by the Examiner. The rejections of claims 1-41 are being appealed.

Further to 37 C.F.R. § 41.37(c)(1)(viii), the attached Claims Appendix contains a clean copy of the pending claims.

IV. STATUS OF AMENDMENTS

The Amendment After Final that was filed on August 4, 2006 ("Amendment After Final"), will be entered for purposes of appeal further to the Advisory Action mailed August 16, 2006 ("Advisory Action").

V. SUMMARY OF CLAIMED SUBJECT MATTER

A. Independent Claim 1

Independent claim 1 is directed to a content management method for managing content data provided to user equipment. An exemplary embodiment of this content management method is described in the Specification at, for example, pg. 14, paragraph 3 to pg. 17, paragraph 3. This embodiment is also illustrated in Figure 5 of the Specification.

B. Independent Claim 20

Independent claim 20 is directed to a content management system for managing content data. An exemplary embodiment of this content management system is described in the Specification at, for example, pg. 14, paragraph 3 to pg. 17, paragraph 3. This embodiment is also illustrated in Figure 5 of the Specification.

The content management system recited in claim 20 comprises the means-plus-function element of "a sending means for sending the encrypted content key and the second storage key to a key management unit." An exemplary embodiment of this "sending means" is described in the Specification at, for example, pg. 15, paragraph 3. This embodiment of the "sending means" is also shown in Figure 5 of the Specification as the "receiver" at reference number 14. An exemplary embodiment of the "key management unit" is shown in Figure 5 as the "key management center" at reference number 13.

Claim 20 further recites the means-plus-function element of "a first decrypting means, in the key management unit, for decrypting the encrypted content key using the first storage key, the first storage key being stored in the key management unit." An exemplary embodiment of this "first decrypting means" is described in the Specification at pg. 15, paragraph 3. This embodiment of the "first decrypting means" is also shown in Figure 5 of the Specification as the "key management center" at reference number 13. An exemplary embodiment of the "key management unit" is also shown in Figure 5 as the "key management center" at reference number 13.

Claim 20 also recites the means-plus-function element of "an encrypting means for encrypting the decrypted content key using the second storage key." An exemplary embodiment of this "encrypting means" is described in the Specification at, for example,

pg. 15, paragraph 3. This embodiment of the "encrypting means" is also shown in Figure 5 of the Specification as the "key management center" at reference number 13.

In addition, claim 20 recites the means-plus-function element of "a second decrypting means for decrypting the encrypted content key using the second storage key and decrypting the content data using the decrypted content key." An embodiment of this "second decrypting means" is described in the Specification at, for example, pg. 16, paragraph 2. This embodiment of the "second decrypting means" is also shown in Figure 5 of the Specification as the "receiver" at reference number 14.

VI. GROUNDS OF REJECTION

A. Claim 1

In the final Office Action mailed June 5, 2006 ("final Office Action"), the Examiner rejected claim 1 under 35 U.S.C. § 101. However, the Examiner withdrew the rejection under 35 U.S.C. § 101 in the Advisory Action.

B. Claims 8, 10, 13, 18, 24-30, 34-37, and 39-41

Claims 8, 10, 13, 18, 24-30, 34-37, and 39-41 stand rejected under 35 U.S.C. § 112, second paragraph, as indefinite for failing to particularly point out and distinctly claim the subject matter which Applicant regards as the invention.

C. Claims 1-41

Claims 1-41 stand rejected under 35 U.S.C. § 102(e) as anticipated by U.S. Patent No. 5,784,464 to Akiyama et al. ("*Akiyama et al.*").

VII. ARGUMENTS

A. § 112, Second Paragraph, Rejection

The rejection of claims 8, 10, 13, 18, 24-30, 34-37, and 39-41 under 35 U.S.C. § 112, second paragraph, as indefinite is improper because these claims particularly point out and distinctly claim the invention.

The requirement that the claims "particularly point[] out and distinctly claim[]" the invention is met when a person experienced in the field of the invention would understand the scope of the subject matter that is patented when the claim is read in conjunction with the rest of the specification. "If the claims when read in light of the specification reasonably apprise those skilled in the art of the scope of the invention, § 112 demands no more." *S3, Inc. v. Nvidia Corp.*, 259 F.3d 1364, 1367, 59 USPQ2d 1745, 1747 (Fed. Cir. 2001) (quoting *Miles Laboratories, Inc. v. Shandon*, 997 F.2d 870, 875, 27 USPQ2d 1123, 1126 (Fed. Cir. 1993).

1. Claims 8, 10, 13, 28, and 34

Claim 8 recites, *inter alia*, "the key management unit generates the second key ... while performing an accounting following a predetermined procedure." Claims 10, 13, 28, and 34 recite similar language for the purposes of the pending appeal.

First, the Examiner argues in the final Office Action, that the recitation in claim 8, at line 6, of "following a predetermined procedure" renders the claim indefinite "since the metes and bounds of predetermined procedure would not be understood by the skilled artisan because such standards are subject to change over time." Final Office Action at pg. 3, paragraph 4. The Examiner applies the same argument to claims 10, 13, 28, and 34. *Id.*

Second, the Examiner argues in relation to claims 8, 13, and 28, "[t]he recitation of 'while' indicates something happening 'during' another event. While, "following" indicates something happens 'after' event. The question remains, how can one event takes [sic] place both 'while' and after all at the same time? Is the procedure identified prior to the performing? or during? Or is the performing taking place following a predetermined procedure and then the accounting is taking place?" Advisory Action at pg. 2, paragraph 4.

Third, the Examiner argues in relation to claims 8, 10, 28, and 34, "the sentence doesn't appear to be complete in order to make grammatical sense, 'performing an accounting' of what? Similarly, the remaining claims fall under the same deficiency." *Id.*

In regard to the Examiner's first argument, the term "predetermined" is an adjective that modifies the noun "procedure" in claims 8, 10, 13, 28, and 34. One of ordinary skill would understand that the term "predetermined procedure" does not refer to any particular procedure, as apparently understood by the Examiner. Rather, one of ordinary skill would understand that "predetermined procedure" refers to a procedure that has been "determined" at a prior time. One of ordinary skill would understand that the adjective "predetermined" does not refer, for example, to a procedure whose "metes and bounds" are "subject to change over time."

In regard to the Examiner's second argument, one of ordinary skill would understand that the phrase "following [a/the] predetermined procedure" in claims 8, 13, and 28 means "according to [a/the] predetermined procedure." For example, The Merriam-Webster Online Dictionary defines "to follow" as, *inter alia*, "to be or act in accordance with <*follow* directions>." "[F]ollowing [a/the] predetermined procedure," in

the context of claims 8, 13, and 28, clearly does not refer to something coming afterwards in time as incorrectly read by the Examiner. Rather, this phrase means "according to [a/the] predetermined procedure."

In regard to the Examiner's third argument, one of ordinary skill would understand that "performing an accounting" refers to creating a record. Furthermore, claims 8, 10, 28, and 34 recite that the accounting is performed "following a predetermined procedure." Thus, is it not necessary for the phrase "performing an accounting" to additionally refer to a particular type of record in order to render this phrase to be definite under § 112, second paragraph.

2. Claims 8, 28, and 34

In the final Office Action at pg. 3, paragraph 6, the Examiner alleges that claims 8, 28, and 34 have insufficient antecedent basis for a recitation of "the data service" at line 5. In the Amendment After Final, claims 8, 28, and 34 were amended to correct informalities, which included deleting the term "the data service" in these claims. Since the Examiner does not repeat this rejection on this particular ground in the Advisory Action, it appears that this rejection of claims 8, 28, and 34 on this ground has been obviated.

3. Claims 18 and 41

Claims 18 and 41 recite, "the content key has added thereto frequency information that limits the number of times the content key can be used" (emphasis added).

In the final Office Action at pg. 4, paragraph 1, the Examiner alleges that claims 18 and 41 have insufficient antecedent basis for a recitation of "the number of times."

However, the rejection of claims 18 and 41 on this ground is improper for at least the reason that the phrase "the number of times the content key can be used," recited in claims 18 and 41, is an inherent component of the "content key" that is also recited in claims 18 and 41.

"[T]he failure to provide explicit antecedent basis for terms does not always render a claim indefinite. If the scope of a claim would be reasonably ascertainable by those skilled in the art, then the claim is not indefinite. *Ex parte Porter*, 25 USPQ2d 1144, 1145 (Bd. Pat. App. & Inter. 1992) ('controlled stream of fluid' provided reasonable antecedent basis for 'the controlled fluid'). Inherent components of elements recited have antecedent basis in the recitation of the components themselves. For example, the limitation 'the outer surface of said sphere' would not require an antecedent recitation that the sphere has an outer surface. See *Bose Corp. v. JBL, Inc.*, 274 F.3d 1354, 1359, 61 USPQ2d 1216, 1218-19 (Fed. Cir 2001) (holding that recitation of 'an ellipse' provided antecedent basis for 'an ellipse having a major diameter' because '[t]here can be no dispute that mathematically an inherent characteristic of an ellipse is a major diameter')." M.P.E.P. § 2173.05(e) (emphasis added).

The recitation in claims 18 and 41 that the content key "can be used" (emphasis added) has explicit antecedent basis. For example, claim 18 depends from claim 1, which recites, "at the user equipment, decrypting the encrypted content key using the second storage key and decrypting the content data using the decrypted content key" (emphasis added). Similarly, claim 41 depends from claim 20, which recites, "a second decrypting means for decrypting the encrypted content key using the second storage

key and decrypting the content data using the decrypted content key" (emphasis added).

Furthermore, an inherent component of "using the ... content key" is that the content key is "used" a particular "number of times" (emphasis added). In other words, inherent in "using" the content key is that, after using the content key, the content key has been "used" a "number of times" that is one greater than the number of times the content key had previously been used. Thus, there is inherent antecedent basis for the recitation of "the number of times" in claims 18 and 41.

4. Claims 24, 25, 27, 29, and 30

In the final Office Action at pg. 4, paragraph 2, the Examiner alleges that claims 24, 25, 27, 29, and 30 have insufficient antecedent basis for a recitation of "the data storage." However, the rejection of claims 24, 25, 27, 29, and 30 on this ground is improper for at least the reason that claim 24 recites, "the storing means, first decrypting means, and encrypting means form together a data storage" (emphasis added), and claims 25, 27, 29, and 30 depend from claim 24.

The term "the data storage" in claim 24 properly refers back to the term "a data storage" that is recited earlier in claim 24. Similarly, the term "the data storage" in claims 25, 27, 29, and 30 properly refers back to the term "a data storage" that is recited in claim 24, from which claims 25, 27, 29, and 30 depend.

5. Claim 26

In the final Office Action at pg. 4, paragraph 3, the Examiner alleges that claim 26 has insufficient antecedent basis for a recitation of "the second content storing means." In the Amendment After Final, claim 26 was amended to correct informalities, which

included amending the term "the second content storing means" to the term "the storing means" in this claim. Since the Examiner does not repeat this rejection on this particular ground in the Advisory Action, it appears that this rejection of claim 26 on this ground was obviated.

6. Claims 27-30, 35-37, 39, and 40

In the final Office Action at pg. 4, paragraph 4, the Examiner alleges that claims 27-30, 35-37, 39, and 40 have insufficient antecedent basis for a recitation of "the second storing means." In the Amendment After Final, claims 27-30, 35-37, 39, and 40 were amended to correct informalities, which included amending the term "the second storing means" to the term "the storing means" in these claims. Since the Examiner does not repeat this rejection on this particular ground in the Advisory Action, it appears that this rejection of claims 27-30, 35-37, 39, and 40 on this ground was obviated.

7. Claim 30

In the final Office Action at pg. 4, paragraph 5, the Examiner alleges that claim 30 has insufficient antecedent basis for a recitation of "the result of the inspection."

First, the Examiner misquotes claim 30 in the final Office Action. Claim 30 does not recite "the result of the inspection." Rather, claim 30 recites, "the data storage starts decrypting the content key stored in the storing means depending on the result of inspection of the identification information of the data storage, stored in the storing means" (emphasis added). Thus, since "inspection" is introduced in claim 30 without a definite article, claim 30 does not have insufficient antecedent basis for the term "inspection."

Furthermore, there is inherent antecedent basis for the term "the result of inspection" in the term "inspection," because a result is an inherent component of an inspection. As explained above, "[i]nherent components of elements recited have antecedent basis in the recitation of the components themselves." M.P.E.P. § 2173.05(e). Thus, since a "result" inheres in an inspection, there is inherent antecedent basis in claim 30 for the term "the result of inspection."

8. Claim 40

Claim 40 recites, "the content key obtained by decryption from the storing means has added thereto information that the content key has been obtained by restoration, as requirement information."

In the final Office Action at pg. 4, paragraph 6, the Examiner alleges that claim 40 is vague and confusing since the Examiner it not sure what is being referenced by the recitation of the phrase "as requirement information" in this claim.

However, the rejection is improper in relation to claim 40 because one of ordinary skill would understand from reading claim 40, in light of the rest of the Specification, that the "requirement information" clearly refers to the "information" that is recited earlier in claim 40. According to claim 40, the content key has "added thereto" the recited "information." Furthermore, the Specification describes at, for example, the paragraph bridging pp. 27 and 28 that "the receiver 14 can add, to the ... restored content key, information that the content key is a restored one." Thus, the recitation of the "requirement information" in claim 40 is not vague and confusing.

For the reasons explained above, Appellants request that the rejection of claims 8, 10, 13, 18, 24-30, 34-37, and 39-41 under 35 U.S.C. § 112, second paragraph, be reversed.

B. § 102(e) Rejection over *Akiyama et al.*

The rejection of claims 1-41 under 35 U.S.C. § 102(e) as anticipated by *Akiyama et al.* is improper because *Akiyama et al.* fails to disclose each and every element of the rejected claims. To properly anticipate Appellants' claims under 35 U.S.C. § 102, each and every element as set forth in the claim must be found, either expressly or inherently described, in a single prior art reference. M.P.E.P. § 2131.

1. Claims 1-19

Claims 1-19 are not anticipated by *Akiyama et al.* for at least the reason that *Akiyama et al.* does not disclose each and every element of the "content management method" recited in independent claim 1, from which claims 2-19 depend.

In the final Office Action and the Advisory Action, the Examiner fails to clearly explain the pertinence of *Akiyama et al.* to the claim limitations. "When a reference is complex or shows or describes inventions other than that claimed by the applicant, the particular part relied on must be designated as nearly as practicable. The pertinence of each reference, if not apparent, must be clearly explained ..." 37 C.F.R. § 1.104(c)(2). For example, the Examiner fails to clearly point out which element taught by *Akiyama et al.* allegedly constitutes the "content key" recited in claim 1 (emphasis added). Similarly, the Examiner has not clearly pointed out the correspondence between the elements taught by *Akiyama et al.* and any of the "first storage key," "content data," and "second storage key" recited in claim 1 (emphasis added). Thus, Appellants are only

able to address the Examiner's rejection as it has been incompletely explicated in the final Office Action and the Advisory Action.

Akiyama et al. discloses: "a client authenticating system in a data distributing system having a data supplying apparatus for holding data and a client receiving the data distributed via a communication interface from the data supplying apparatus." *Akiyama et al.* at col. 2, lines 46-49. The data supplying apparatus includes "a first data file 12" and "a second data file 13." *Id.* at col. 6, lines 49-51. "The first data file 12 is a database stored with a multiplicity of encrypted contents and IDs (title IDs) thereof. The second data file 13 is a database stored with a multiplicity of re-encrypted contents which had been stored in the first data file 12 and re-encrypted by use of a different key and with title IDs thereof." *Id.* at col. 7, lines 1-6. To carry out a content data distributing process, "the service provider system 1 reads a content (encrypted content) corresponding to the title ID (IDT) requested from the service client 6 from one of the data files 12, 13 and decrypts this content. Then, the decrypted content is transmitted via the S1 interface to the service client 6." *Id.* at col. 13, lines 15-21.

Akiyama et al. further discloses: "the service provider system 1, as shown in FIG. 8, distributes a key (KG_j) for decrypting the encrypted content which is referred to as a title key. The title key is distributed via the S2 interface to smoothly decrypt the data of a variety of content on the side of the service client 6. That is, the service provider system 1 generates a client individual key K_i from the MASC identification ID (ID_i) transmitted by the MASC 5 attached to the service client 6 (the key used for authenticating the client may also be diverted as the client individual key K_i). The service provider system 1 encrypts a service provider ID (IDP) and a title key KG_{1j} with

the client individual key K_i. ... An item of encrypted key data from the service provider system 1 is decrypted in the MASC 5, thereby the title key KG_{1j} is obtained. Thereafter, the encrypted contents transmitted via the S1 interface are to be decrypted with this title key KG_j." *Id.* at col. 14, lines 7-28.

a. The "content key" recited in claim 1 does not read on the "contents" or "title ID" of *Akiyama et al.*

The Examiner alleges, "Akiyama teaches encrypting content with a content key, and later encrypting the content key with yet another key, specifically, in column 7, lines 1-11, where he recites: The first data file 12 is a database stored with a multiplicity of encrypted contents and IDs (title IDs) thereof. The second data file 13 is a database stored with a multiplicity of re-encrypted contents which had been stored in the first data file 12 and re-encrypted by use of a different key and with title IDs thereof." Advisory Action at pg. 2, paragraph 6. Although unclear from the Examiner's explication, it appears that the Examiner relies on either the "contents" or the "title IDs" of *Akiyama et al.* as allegedly constituting the "content key" recited in claim 1.

However, the claimed "content key" does not read on either the "contents" or the "title IDs" of *Akiyama et al.* for at least the reason that *Akiyama et al.* fails to teach "storing a content key encrypted with a first storage key, content data encrypted with the content key, and a second storage key," as required by claim 1.

Neither the "contents" that are encrypted and stored in the first data file (12) of *Akiyama et al.*, nor the "contents" that are encrypted and stored in the second data file (13) of *Akiyama et al.*, constitute the "content key" recited in claim 1. For example, *Akiyama et al.* is silent on the matter of "content data encrypted with" the contents, as

required by claim 1 (emphasis added). Thus, the "contents" of *Akiyama et al.* do not constitute the "content key" recited in claim 1.

The "title IDs" of *Akiyama et al.* also do not constitute the "content key encrypted with a first storage key," as recited in claim 1, for at least the reason that the title IDs of *Akiyama et al.* are never encrypted. Although *Akiyama et al.* teaches storing encrypted contents in the first and second data files (12, 13), and additionally teaching storing the title IDs in the first and second data files (12, 13), the title IDs remain unencrypted.

For example, *Akiyama et al.* teaches at col. 13, lines 16-20, "the service provider system 1 reads a content (encrypted content) corresponding to the title ID (IDT) requested from the service client 6 from one of the data files 12, 13 and decrypts this content." If the title IDs corresponding to the contents were encrypted together with the contents before being stored in the first data file (12), then the service provider system (1) would not be able to determine which encrypted content corresponds to the requested title ID from the service client (6) without first decrypting the title IDs and the content that are stored in the first data file (12). However, *Akiyama et al.* teaches decrypting the content only after it is determined which content corresponds to the requested title ID.

b. The "content key" recited in claim 1 does not read on the "title key" of *Akiyama et al.*

In the Advisory Action, the Examiner includes a new ground of rejection that was not alleged in the final Office Action. The Examiner asserts that *Akiyama et al.* teaches "distribut[ing] a key (KG.sub.j) for decrypting the encrypted content which is referred to as a title key. The title key is distributed via the S2 interface to smoothly decrypt the

data of a variety of content on the side of the service client 6." Advisory Action at pg. 2, paragraph 6.

However, the "title key" of *Akiyama et al.* also does not constitute the "content key" recited in claim 1. For example, *Akiyama et al.* fails to teach "decrypting the encrypted content key using [a] first storage key," "encrypting the decrypted content key using [a] second storage key," and "decrypting the encrypted content key using the second storage key," as required by claim 1.

Rather, the service provider (1) encrypts the title key KG_{ij} using the client individual key K_i. *Akiyama et al.* at col. 14, lines 16-18. In the MASC (5), the title key KG_{ij} is decrypted. *Id.* at col. 14, lines 24-26. However, encrypting and decrypting the title key KG_{ij} using a single key K_i does not constitute decrypting a content key using a first storage key, encrypting the content key using a second storage key, and decrypting the content key using the second storage key, as required by claim 1.

Thus, since *Akiyama et al.* does not disclose each and every element of independent claim 1, Appellants request that the rejection of claim 1 and claims 2-19, which depend therefrom, over *Akiyama et al.* under 35 U.S.C. § 102(e) be reversed.

2. Claims 20-41

Claims 20-41 are not anticipated by *Akiyama et al.* for at least the reason that *Akiyama et al.* does not disclose each and every element of the "content management system" recited in independent claim 20, from which claims 21-41 depend.

a. The "content key" recited in claim 20 does not read on the "contents" or "title ID" of *Akiyama et al.*

The "content key" recited in claims 20-41 does not read on either the "contents" or the "title IDs" of *Akiyama et al.* for at least the reason that *Akiyama et al.* fails to teach "a storing means having stored therein a content key encrypted with a first storage key, content data encrypted with the content key, and a second storage key," as required by claim 20.

As explained in relation to claim 1, neither the "contents" that are encrypted and stored in the first data file (12) of *Akiyama et al.*, nor the "contents" that are encrypted and stored in the second data file (13) of *Akiyama et al.*, constitute the "content key" recited in claim 20. For example, *Akiyama et al.* is silent on the matter of "content data encrypted with" the contents, as would be required by claim 20 (emphasis added).

The "title IDs" of *Akiyama et al.* also do not constitute the "content key encrypted with a first storage key," as recited in claim 20, for at least the reason that the title IDs of *Akiyama et al.* are never encrypted. Although the title IDs are stored in the first and second data files (12, 13) together with the encrypted contents, the title IDs remain unencrypted.

b. The "content key" recited in claim 20 does not read on the "title key" of *Akiyama et al.*

As explained in relation to claim 1, the "title key" of *Akiyama et al.* also does not constitute the "content key" recited in claim 20. For example, *Akiyama et al.* fails to teach "a first decrypting means ... for decrypting the encrypted content key using [a] first storage key," "an encrypting means for encrypting the decrypted content key using [a]

second storage key," and "a second decrypting means for decrypting the encrypted content key using the second storage key," as required by claim 20.

Encrypting and decrypting a title key KG_{ij} using a single key K_i, as in *Akiyama et al.*, does not constitute decrypting a content key using a first storage key, encrypting the content key using a second storage key, and decrypting the content key using the second storage key, as required by claim 20.

Thus, since *Akiyama et al.* does not disclose each and every element of independent claim 20, Appellants request that the rejection of claim 20 and claims 21-41, which depend therefrom, over *Akiyama et al.* under 35 U.S.C. § 102(e) be reversed.

VIII. CONCLUSION

For the reasons given above, pending claims 1-41 are allowable and reversal of the Examiner's rejection is respectfully requested.

To the extent any extension of time under 37 C.F.R. § 1.136 is required to obtain entry of this Appeal Brief, such extension is hereby respectfully requested. If there are any fees due under 37 C.F.R. §§ 1.16 or 1.17 that are not enclosed herewith, including any fees required for an extension of time under 37 C.F.R. § 1.136, please charge such fees to our Deposit Account No. 06-0916.

Respectfully submitted,

FINNEGAN, HENDERSON, FARABOW,
GARRETT & DUNNER, L.L.P.

Dated: November 3, 2006

By: _____
Reece Nienstadt
Reg. No. 52,072

IX. CLAIMS APPENDIX TO APPEAL BRIEF UNDER RULE 41.37(C)(1)(VIII)

1. A content management method for managing content data provided to user equipment, comprising the steps of:

storing a content key encrypted with a first storage key, content data encrypted with the content key, and a second storage key in the user equipment;

sending the encrypted content key and the second storage key to a key management unit;

at the key management unit, decrypting the encrypted content key using the first storage key, the first storage key being stored in the key management unit; and

encrypting the decrypted content key using the second storage key;

sending the content key encrypted with the second storage key along with the encrypted content to the user equipment; and

at the user equipment, decrypting the encrypted content key using the second storage key and decrypting the content data using the decrypted content key.

2. The method as set forth in Claim 1, wherein the second storage key is generated based on a random number.

3. The method as set forth in Claim 1, wherein the decrypted content key is encrypted with identification information of the user equipment and stored into the user equipment.

4. The method as set forth in Claim 1, wherein the content key is encrypted, in the user equipment, with the first storage key and identification information of the user equipment, and the content key stored in the user equipment is decrypted with the first storage key and the identification information of the user equipment.

5. The method as set forth in Claim 1, wherein the second storage key is generated by a decrypted key generating means provided in the user equipment.

6. The method as set forth in Claim 5, wherein the second storage key is encrypted with a public key for the key management unit for management of the storage keys to generate a third storage key and the third storage key is stored into the user equipment.

7. The method as set forth in Claim 6, wherein the user equipment deletes the second storage key depending upon whether the third storage key has been stored in the user equipment.

8. The method as set forth in Claim 7, wherein, when decrypting the content key stored in the user equipment, the user equipment sends the third storage key to the key management unit; and the key management unit generates the second storage key based on the third storage key while performing an accounting following a predetermined procedure.

9. The method as set forth in Claim 1, wherein the second storage key is generated by a storage key generating means provided in the key management unit which manages the storage keys; and the key management unit has stored therein the second storage key and identification information of the user equipment in which the content key encrypted with the above generated second storage key is stored.

10. The method as set forth in Claim 9, wherein upon the generation of the second storage key, the key management unit performs an accounting following a predetermined procedure.

11. The method as set forth in Claim 9, wherein the key management unit encrypts the second storage key with the management key to generate a third storage key, and sends the third storage key to the user equipment; and the user equipment stores the received third storage key.

12. The method as set forth in Claim 11, wherein the user equipment deletes the second storage key depending upon whether the third storage key has been stored.

13. The method as set forth in Claim 12, wherein the key management unit has stored therein the identification information of the user equipment in which the content key encrypted with the second storage key is stored; the user equipment sends, when decrypting the content key stored in the user equipment, the identification information of the user equipment to the key management unit; and the key

management unit generates the second storage key based on the result of comparison between identification information of the user equipment, sent from the user equipment, and the identification information of the user equipment, held in the key management unit itself, while accounting the data service following the predetermined procedure.

14. The method as set forth in Claim 1, wherein the user equipment has stored therein identification information of the user equipment.

15. The method as set forth in Claim 14, wherein the user equipment starts decrypting the content key stored in the user equipment depending upon the result of an inspection of the identification information of the user equipment, stored in the user equipment.

16. The method as set forth in Claim 1, wherein the decrypted content key supplied from the user equipment has added thereto information that the content key has been obtained by restoration.

17. The method as set forth in Claim 16, wherein when moving the content key having added thereto the information that the content key has been obtained by restoration, the user equipment performs an error process based on the result of comparison between the content key and another content key stored in a destination to which the content key is to be moved.

18. The method as set forth in Claim 1, wherein the content key has added thereto frequency information that limits the number of times the content key can be used.

19. The method as set forth in Claim 1, further comprising storing the content key encrypted with the second storage key in a first storage of the user equipment along with identification information of the first storage; storing the content key that is stored in the first storage, and the identification information of the first storage, into a second storage of the user equipment; and performing, when a request is made to decrypt the content key in the first storage, an error process based on the result of comparison between the identification information of the first storage and the identification information of the second storage.

20. A content management system for managing content data, comprising:

a storing means having stored therein a content key encrypted with a first storage key, content data encrypted with the content key, and a second storage key;

a sending means for sending the encrypted content key and the second storage key to a key management unit;

a first decrypting means, in the key management unit, for decrypting the encrypted content key using the first storage key, the first storage key being stored in the key management unit;

an encrypting means for encrypting the decrypted content key using the second storage key; and

a second decrypting means for decrypting the encrypted content key using the second storage key and decrypting the content data using the decrypted content key.

21. The system as set forth in Claim 20, further comprising storage key generating means for generating the second storage key by means of a random number generator.

22. The system as set forth in Claim 20, wherein the encrypting means encrypts the decrypted content key with identification information of the storing means.

23. The system as set forth in Claim 20, wherein the content key is encrypted, in the storing means, with the first storage key and identification information of the storing means; and the content key stored in the storing means is decrypted with the first storage key and the identification information of the storing means.

24. The system as set forth in Claim 20, wherein the storing means, first decrypting means, and encrypting means form together a data storage, and wherein the key management unit manages the second storage key of the data storage.

25. The system as set forth in Claim 24, wherein the data storage is a data receiver that receives a content data encrypted and sent from a data transmitter.

26. The system as set forth in Claim 24, further comprising means for storing a public key of the key management unit; and wherein the storing means has stored therein the second storage key along with a third storage key obtained by encrypting the second storage key with the public key.

27. The system as set forth in Claim 26, wherein the data storage deletes the second storage key depending upon whether the third storage key is stored in the storing means.

28. The system as set forth in Claim 27, wherein, when decrypting the content key stored in the storing means, the data storage sends the third storage key to the key management unit; and the key management unit sends the second storage key generated based on the third storage key to a data transmitter while performing an accounting following a predetermined procedure.

29. The system as set forth in Claim 24, wherein the storing means has stored therein identification information of the data storage.

30. The system as set forth in Claim 29, wherein the data storage starts decrypting the content key stored in the storing means depending on the result of inspection of the identification information of the data storage, stored in the storing means.

31. The system as set forth in Claim 20, wherein the storing means, first decrypting means, and encrypting means form together a data storage; and further comprising a storage key generating means, wherein the key management unit manages the second storage key of the data storage.

32. The system as set forth in Claim 31, wherein the data storage is a data receiver that receives a content data encrypted and sent from a data transmitter.

33. The system as set forth in Claim 31, wherein the key management unit comprises an identification information storing means in which identification information of the storing means is stored.

34. The system as set forth in Claim 31, wherein the key management unit performs an accounting following a predetermined procedure depending upon a generation of the second storage key.

35. The system as set forth in Claim 31, wherein the key management unit comprises means for storing storage keys; the key management unit generates a third storage key by encrypting the second storage key with a management key and sends the third storage key to the data storage; and the data storage stores the third storage key into the storing means.

36. The system as set forth in Claim 35, wherein the data storage deletes the second storage key depending upon whether the third storage key is stored in the storing means.

37. The system as set forth in Claim 36, wherein the key management unit comprises means for storing the second storage key and identification information of the storing means in which the content key encrypted with the second storage key is stored; the key management unit performs an accounting, when the data storage decrypts the content key, following a predetermined procedure based on the result of comparison between the identification information of the storing means, sent from the data storage, and identification information stored in an identification information storing means.

38. The system as set forth in Claim 31, wherein the storing means has stored therein identification information of the data storage.

39. The system as set forth in Claim 38, wherein the data storage starts decrypting the content key stored in the storing means.

40. The system as set forth in Claim 20, wherein the content key obtained by decryption from the storing means has added thereto information that the content key has been obtained by restoration, as requirement information.

41. The system as set forth in Claim 20, wherein the content key has added thereto frequency information that limits the number of times the content key can be used.

X. EVIDENCE APPENDIX TO APPEAL BRIEF UNDER RULE 41.37(C)(1)(IX)

Appellants do not rely, in the pending appeal, upon any evidence referred to in 37 C.F.R. § 41.37(c)(1)(ix).

XI. RELATED PROCEEDINGS APPENDIX TO APPEAL BRIEF UNDER RULE 41.37(C)(1)(X)

There are currently no other proceedings, of which Appellants, Appellants' legal representative, or Assignee are aware, that will directly affect or be directly affected by or have a bearing on the Board's decision in the pending appeal.